

DIALOG(R)File 351:Derwent WPI
(c) 2008 The Thomson Corporation. All rts. reserv.

0011243513

WPI ACC NO: 2002-183303/

XRPX Acc No: N2002-139489

Communication condition control method in internet, involves canceling data transmitted to server, when measured amount of data exceeds preset regulation value

Patent Assignee: NTT COMMUNICATIONS KK (NITE)

Inventor: AIHARA T

1 patents, 1 countries

Patent Family

Patent			Application			
Number	Kind	Date	Number	Kind	Date	Update
JP 2002016633	A	20020118	JP 2000199565	A	20000630	200224 B

Priority Applications (no., kind, date): JP 2000199565 A 20000630

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
JP 2002016633	A	JA	10	6	

Alerting Abstract JP A

NOVELTY - A user's server is connected to circuit router through internet. The quantity of data transmitted to the server from the transmitting element having specific IP address, is measured. When measured amount of data exceeds preset regulation value, the data transmitted to the server is canceled.

DESCRIPTION - An INDEPENDENT CLAIM is also included for communication condition control system.

USE - For controlling communication between individual and enterprise through internet.

ADVANTAGE - User's server connected to ISP can be protected from irregular access, by canceling the data being transmitted for more than fixed quantity in ISP.

DESCRIPTION OF DRAWINGS - The figure shows the block diagram of communication condition control system. (Drawing includes non-English language text).

Basic Derwent Week: *200224*

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-16633

(P2002-16633A)

(43) 公開日 平成14年1月18日 (2002.1.18)

(51) Int.Cl.⁷

H 0 4 L 12/56

識別記号

F I

H 0 4 L 11/20

テーマコード(参考)

1 0 2 E 5 K 0 3 0

審査請求 未請求 請求項の数13 O L (全 10 頁)

(21) 出願番号 特願2000-199565 (P2000-199565)

(22) 出願日 平成12年6月30日 (2000.6.30)

(71) 出願人 399035766

エヌ・ティ・ティ・コミュニケーションズ
株式会社

東京都千代田区内幸町一丁目1番6号

(72) 発明者 相原 俊幸

東京都千代田区内幸町一丁目1番6号 エ
ヌ・ティ・ティ・コミュニケーションズ株
式会社内

(74) 代理人 100064621

弁理士 山川 政樹

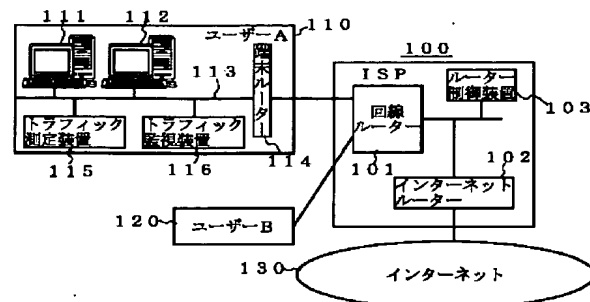
Fターム(参考) 5K030 GA13 HD03 HD08 LC11 LC15
MB09

(54) 【発明の名称】 通信状態制御方法および通信状態制御システム

(57) 【要約】

【課題】 大量のデータを送信してくる不正アクセスから、ISPに接続されているユーザーのサーバーを守る。

【解決手段】 トラフィック測定装置115は、ネットワーク113の状態を監視し、トラフィック監視装置116が、監視の結果検出された輻輳状態などを判定してルーター制御装置103に通知する。また、トラフィック監視装置116からの通知により、ルーター制御装置103は、回線ルーター101やインターネットルーター102を制御し、ルーター制御装置103から通知されたIPアドレスからのデータを破棄させる。



1

【特許請求の範囲】

【請求項1】 インターネット側に接続したインターネットルーターと、このインターネットルーターに接続する回線ルーターとを備えたインターネットサービスプロバイダを介し、ユーザーのサーバーを専用線で前記回線ルーターに接続して前記サーバーを前記インターネットに接続し、

前記サーバーに対して前記インターネットを介して送信されたデータの量と、このデータを送信してきた送信元のIPアドレスとを所定時間毎に測定し、

測定したデータ量が予め設定されている規定値以上となった場合、規定値以上のデータ量を送信してきた特定送信元の特定IPアドレスから前記サーバーに対して送信されてきたデータは、前記インターネットルーターまたは前記回線ルーターのいずれか一方もしくは両方に破棄させることを特徴とする通信状態制御方法。

【請求項2】 請求項1記載の通信状態制御方法において、

前記サーバーに対して前記インターネットを介して送信されたデータの量と、このデータを送信してきた送信元のIPアドレスとの測定は、前記ユーザー側で行い、前記ユーザー側で測定したデータ量が予め設定されている規定値以上になったと判断されたとき、前記インターネットサービスプロバイダ側で前記特定IPアドレスから前記サーバーに対して送信されてきたデータを、前記インターネットルーターまたは前記回線ルーターのいずれか一方もしくは両方に破棄させることを特徴とする通信制御方法。

【請求項3】 インターネット側に接続したインターネットルーターと、このインターネットルーターに接続する回線ルーターとを備えたインターネットサービスプロバイダを介し、ユーザーのサーバーを専用線で前記回線ルーターに接続して前記サーバーを前記インターネットに接続し、

前記サーバーのCPUの稼働率とこのCPUの主メモリの使用率と前記サーバーに対する一定時間あたりの総リクエスト数と単位時間あたりの通信量とを測定し、前記稼働率と使用率と総リクエスト数と通信量とが予め設定されている規定値以上となった場合、規定値以上となった時点においてデータを送信していた特定送信元の特定IPアドレスから前記サーバーに対して送信されてきたデータは、前記インターネットルーターまたは前記回線ルーターのいずれか一方もしくは両方に破棄させることを特徴とする通信状態制御方法。

【請求項4】 請求項3記載の通信状態制御方法において、

前記サーバーのCPUの稼働率とこのCPUの主メモリの使用率と前記サーバーに対する一定時間あたりの総リクエスト数と単位時間あたりの通信量とを測定は、前記ユーザー側で行い、

2

前記ユーザー側で前記稼働率と使用率と総リクエスト数と通信量とが予め設定されている規定値以上になったと判断されたとき、前記インターネットサービスプロバイダ側で前記特定IPアドレスから前記サーバーに対して送信されてきたデータを、前記インターネットルーターまたは前記回線ルーターのいずれか一方もしくは両方に破棄させることを特徴とする通信制御方法。

【請求項5】 請求項1～4いずれか1項記載の通信状態制御方法において、

10 前記サーバーは、このサーバーが接続するネットワークを介して前記専用線に接続し、前記ネットワークは端末ルーターを介して前記専用線に接続することを特徴とする通信状態制御方法。

【請求項6】 請求項1～5いずれか1項に記載の通信状態制御方法において、

前記インターネットルーターまたは前記回線ルーターのいずれか一方もしくは両方で破棄するデータ量が予め設定されている規定値以下となった場合、前記インターネットルーターまたは前記回線ルーターのいずれか一方もしくは両方における前記特定IPアドレスから前記サーバーに対して送信されたデータの破棄を停止することを特徴とする通信状態制御方法。

【請求項7】 インターネット側に接続されたインターネットルーター、このインターネットルーターに接続された回線ルーター、前記インターネットルーターおよび回線ルーターに接続されて前記インターネットルーターおよび回線ルーターを制御するルーター制御装置を備えたインターネットサービスプロバイダと、

30 前記回線ルーターに専用線で接続されたユーザーのサーバーと、このサーバーに対して前記インターネットを介して送信されたデータの量と、このデータを送信してきた送信元のIPアドレスとを所定時間毎に測定するトラフィック測定装置と、

このトラフィック測定装置が測定したデータ量を監視してこのデータ量が予め設定されている規定値以上となった場合、規定値以上のデータ量を送信してきた特定送信元の特定IPアドレスを前記ルーター制御装置に通知するトラフィック監視装置とを備え、

40 前記ルーター制御装置は、前記トラフィック監視装置から通知された特定IPアドレスから前記サーバーに対して送信されてきたデータを、前記インターネットルーターまたは前記回線ルーターのいずれか一方もしくは両方に破棄させるように制御することを特徴とする通信状態制御システム。

【請求項8】 インターネット側に接続されたインターネットルーター、このインターネットルーターに接続された回線ルーター、前記インターネットルーターおよび回線ルーターに接続されて前記インターネットルーターおよび回線ルーターを制御するルーター制御装置を備え

3

たインターネットサービスプロバイダと、
前記回線ルーターに専用線で接続するユーザーのサーバと、

このサーバのCPUの稼働率とこのCPUの主メモリの使用率と前記サーバに対する一定時間あたりの総リクエスト数と単位時間あたりの通信量とを測定するトラフィック測定装置と、

前記稼働率と使用率と総リクエスト数と通信量とを監視してこれらが予め設定されている規定値以上となった場合、規定値以上となった時点においてデータを送信していた特定送信元の特定IPアドレスを前記ルーター制御装置に通知するトラフィック監視装置とを備え、
前記ルーター制御装置は、前記トラフィック監視装置から通知された特定IPアドレスから前記サーバに対して送信されてきたデータを前記インターネットルーターまたは前記回線ルーターのいずれか一方もしくは両方に破棄させるように制御することを特徴とする通信状態制御システム。

【請求項9】 請求項7または8記載の通信状態制御システムにおいて、

前記サーバが接続するネットワークと、
このネットワークと前記専用線とを接続する端末ルーターとを備えたことを特徴とする通信状態制御システム。

【請求項10】 請求項7～9いずれか1項に記載の通信状態制御システムにおいて、

前記ルーター制御装置は、前記インターネットルーターまたは前記回線ルーターのいずれか一方もしくは両方で破棄するデータ量が予め設定されている規定値以下となった場合、前記インターネットルーターまたは前記回線ルーターのいずれか一方もしくは両方における前記特定IPアドレスから前記サーバに対して送信されたデータの破棄を停止するように制御することを特徴とする通信状態制御システム。

【請求項11】 ユーザー側のネットワークに対してトラフィックを渡す回線ルータと、この回線ルータと通信ネットワークを介して接続されてインターネットからの前記ユーザー側のネットワークへのトラフィックを受け取るインターネットルータとを有するネットワークにおける通信状態制御方法であって、

前記ユーザー側のネットワークから、特定のIPアドレスからのトラフィックについての制御指示を受け取ると、
前記ユーザーに対応付けて予め登録してある制御内容にしたがって前記回線ルータとインターネットルータとに対してトラフィック配送の制御を行わせることを特徴とする通信状態制御方法。

【請求項12】 請求項11記載の通信状態制御方法において、

前記ユーザー側のネットワークからの制御信号は、前記ユーザー側のネットワークが受け取るトラフィック量が予め定めた閾値を越えた際に発せられるものであること

4

を特徴とする通信状態制御方法。

【請求項13】 請求項11記載の通信状態制御方法において、

前記ユーザー側のネットワークからの制御指示は、前記ユーザー側のネットワーク内に設置されたサーバのシステム稼働率が予め定められた閾値を越えた際に発せられたものであることを特徴とする通信状態制御方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、インターネットサービスプロバイダを介してインターネットに接続するときの通信状態制御方法および通信状態制御システムに関する。

【0002】

【従来の技術】インターネットにおいて、個人や企業がWebサーバなど公開サーバを運用する場合、インターネットサービスプロバイダ（ISP：Internet Service Provider）を介して、自身のネットワークをインターネットに接続するようにしている。このISPによるインターネットへの接続に関して説明すると、図6に示すように、まず、ISP600は、回線ルーター601とインターネットルーター602とルーター制御装置603とを備えている。回線ルーター601には、ISP600を利用してインターネットに接続しようとするユーザーA610、ユーザーB620からの回線が接続され、インターネットルーター602は、インターネット630に接続される。

【0003】一方、ユーザーA610は、ホームページのHTMLなどが格納されたWebサーバ611や、メールサーバ612などを備え、これらをネットワーク613に接続している。ユーザーA610は、ネットワーク613に端末ルーター614を設け、回線641を介してISP600の回線ルーター601に接続している。この構成では、インターネット630に接続している他端末650とユーザーA610のWebサーバ611は、端末ルーター614－回線ルーター601－インターネットルーター602の経路で、インターネット630を介して接続された状態となる。これらは、ユーザーB620も同様である。したがって、例えば、他端末650からは、Webサーバ611に用意されたホームページが閲覧可能な状態となっている。

【0004】

【発明が解決しようとする課題】ところで、インターネット630に接続している他の端末から、ユーザーA610のWebサーバ611やメールサーバ612に対してデータが送信されてくると、返信のためのデータ送信などの応答処理を行う。ところが、上記他の端末から、これらサーバが処理しきれない大量のデータを送信してくると、Webサーバ611やメールサーバ612は、対応処理が追いつかず、各サーバ内やネッ

5

トワーク613が輻輳状態となる。従来では、このような不正アクセスが発生した場合、ユーザー側で送信されてきたデータに対する応答を停止するなど、ユーザー側のネットワーク内部で対応してきた。このため、上記ネットワーク攻撃が発生すると、ユーザー側では、ネットワークの輻輳による各サーバーの停止状態を抑制できない場合が多かった。

【0005】本発明は、以上のような問題点を解消するためになされたものであり、大量のデータを送信してくる不正アクセスから、ISPに接続されているユーザーのサーバーを守ることを目的とする。

【0006】

【課題を解決するための手段】本発明の通信状態制御方法は、インターネットサービスプロバイダを介してインターネットに接続しているユーザーのサーバーに対してインターネットを介して送信されたデータの量と、このデータを送信してきた送信元のIPアドレスとを所定時間毎に測定し、測定したデータ量が予め設定されている規定値以上となった場合、規定値以上のデータ量を送信してきた特定送信元の特定IPアドレスからサーバーに対して送信されてきたデータは、インターネットルーターまたは回線ルーターのいずれか一方もしくは両方に破棄させようとしたものである。この発明によれば、規定値以上のデータ量を送信してきた送信元からのデータは、ユーザーのサーバーにまで到達しない。

【0007】上記発明では、サーバーに対してインターネットを介して送信されたデータの量と、このデータを送信してきた送信元のIPアドレスとの測定は、ユーザー側で行い、ユーザーで測定したデータ量が予め設定されている規定値以上になったと判断されたとき、インターネットサービスプロバイダ側で特定IPアドレスからサーバーに対して送信されてきたデータを、インターネットルーターまたは回線ルーターのいずれか一方もしくは両方に破棄させる。

【0008】また、本発明の通信状態制御方法は、インターネットサービスプロバイダを介してインターネットに接続しているユーザーのサーバーのCPUの稼働率とこのCPUの主メモリの使用率とサーバーに対する一定時間あたりの総リクエスト数と単位時間あたりの通信量とを測定し、稼働率と使用率と総リクエスト数と通信量とが予め設定されている規定値以上となった場合、規定値以上となった時点においてデータを送信していた特定送信元の特定IPアドレスからサーバーに対して送信されてきたデータは、インターネットルーターまたは回線ルーターのいずれか一方もしくは両方に破棄させようとしたものである。この発明によれば、測定値が規定値以上となった場合の送信元からのデータは、ユーザーのサーバーにまで到達しない。

【0009】上記発明では、サーバーのCPUの稼働率とこのCPUの主メモリの使用率とサーバーに対する一

6

定時間あたりの総リクエスト数と単位時間あたりの通信量とを測定は、ユーザー側で行い、ユーザー側で稼働率と使用率と総リクエスト数と通信量とが予め設定されている規定値以上になったと判断されたとき、インターネットサービスプロバイダ側で特定IPアドレスからサーバーに対して送信されてきたデータを、インターネットルーターまたは回線ルーターのいずれか一方もしくは両方に破棄させる。

【0010】また、上記発明において、サーバーは、このサーバーが接続するネットワークを介して専用線に接続し、ネットワークは端末ルーターを介して専用線に接続する。また、インターネットルーターまたは回線ルーターのいずれか一方もしくは両方で破棄するデータ量が予め設定されている規定値以下となった場合、インターネットルーターまたは回線ルーターのいずれか一方もしくは両方における特定IPアドレスからサーバーに対して送信されたデータの破棄を停止する。

【0011】本発明の通信状態制御システムは、インターネットルーターおよび回線ルーターに接続されてインターネットルーターおよび回線ルーターを制御するルーター制御装置を備えたインターネットサービスプロバイダと、回線ルーターに専用線で接続されたユーザーのサーバーと、このサーバーに対してインターネットを介して送信されたデータの量と、このデータを送信してきた送信元のIPアドレスとを所定時間毎に測定するトラフィック測定装置と、このトラフィック測定装置が測定したデータ量を監視してこのデータ量が予め設定されている規定値以上となった場合、規定値以上のデータ量を送信してきた特定送信元の特定IPアドレスをルーター制御装置に通知するトラフィック監視装置とを備え、ルーター制御装置は、トラフィック監視装置から通知された特定IPアドレスからサーバーに対して送信されてきたデータを、インターネットルーターまたは回線ルーターのいずれか一方もしくは両方に破棄させるように制御するものである。この発明によれば、規定値以上のデータ量を送信してきた送信元からのデータは、ユーザーのサーバーにまで到達しない。

【0012】本発明の通信状態制御システムは、インターネットルーターおよび回線ルーターに接続されてインターネットルーターおよび回線ルーターを制御するルーター制御装置を備えたインターネットサービスプロバイダと、回線ルーターに専用線で接続するユーザーのサーバーと、このサーバーのCPUの稼働率とこのCPUの主メモリの使用率とサーバーに対する一定時間あたりの総リクエスト数と単位時間あたりの通信量とを測定するトラフィック測定装置と、稼働率と使用率と総リクエスト数と通信量とを監視してこれらが予め設定されている規定値以上となった場合、規定値以上となった時点においてデータを送信していた特定送信元の特定IPアドレスをルーター制御装置に通知するトラフィック監視装置

7

とを備え、ルーター制御装置は、トラフィック監視装置から通知された特定IPアドレスからサーバーに対して送信されてきたデータを、インターネットルーターまたは回線ルーターのいずれか一方もしくは両方に破棄させるように制御するものである。この発明によれば、測定値が規定値以上となった場合の送信元からのデータは、ユーザーのサーバーにまで到達しない。

【0013】上記発明では、サーバーが接続するネットワークと、このネットワークと専用線とを接続する端末ルーターとを備えている。また、ルーター制御装置は、インターネットルーターまたは回線ルーターのいずれか一方もしくは両方で破棄するデータ量が予め設定されている規定値以下となった場合、インターネットルーターまたは回線ルーターのいずれか一方もしくは両方における特定IPアドレスからサーバーに対して送信されたデータの破棄を停止するように制御する。

【0014】また、本発明の通信状態制御方法は、ユーザー側のネットワークに対してトラフィックを渡す回線ルーターと、この回線ルーターと通信ネットワークを介して接続されてインターネットからのユーザー側のネットワークへのトラフィックを受け取るインターネットルーターとを有するネットワークにおける通信状態制御方法であって、ユーザー側のネットワークから、特定のIPアドレスからのトラフィックについての制御指示を受け取ると、ユーザーに対応付けて予め登録してある制御内容にしたがって回線ルーターとインターネットルーターとに対してトラフィック配送の制御を行わせようとしたものである。この発明によれば、規定値以上のトラフィックが発生した場合、これの送信元からのデータは、回線ルーターとインターネットルーターとで制限される。

【0015】上記発明において、ユーザー側のネットワークからの制御信号は、ユーザー側のネットワークが受け取るトラフィック量が予め定めた閾値を越えた際に発せられるものである。また、ユーザー側のネットワークからの制御指示は、ユーザー側のネットワーク内に設置されたサーバーのシステム稼働率が予め定められた閾値を越えた際に発せられたものである。

【0016】

【発明の実施の形態】以下、本発明の実施の形態について図を参照して説明する。図1は、本発明の実施の形態における通信状態制御システムの構成を示す構成図である。図1に示すように、まず、ISP100は、回線ルーター101とインターネットルーター102とルーター制御装置103とを備えている。回線ルーター101には、ISP100を利用してインターネットに接続しようとするユーザーA110、ユーザーB120からの回線が接続され、インターネットルーター102は、インターネット130に接続される。

【0017】一方、ユーザーA110は、ホームページのHTMLなどが格納されたWebサーバー111やメ

8

ールサーバー112などを備え、これらをネットワーク113に接続している。また、ユーザーA110は、端末ルーター114を介し、ネットワーク113をISP100すなわち回線ルーター101に接続している。したがって、Webサーバー111やメールサーバー112は、ISP100を介してインターネット130に接続した状態となっている。加えて、ユーザーA110は、トラフィック測定装置115とトラフィック監視装置116とを備えるようにした。なお、ユーザーB120も同様である。

【0018】本実施の形態では、まず、トラフィック測定装置115が、ネットワーク113の状態を監視し、トラフィック監視装置116が、監視の結果検出された輻輳状態などを判定してルーター制御装置103に通知するようにした。また、トラフィック監視装置116からの通知により、ルーター制御装置103が、回線ルーター101やインターネットルーター102を制御し、ルーター制御装置103から通知されたIPアドレスからのデータを破棄させるようにした。なお、上記制御により、通知されたIPアドレスからのデータをユーザーA110に送らないように制御してもよく、また、通知されたIPアドレスからのデータは、データ量を削減してユーザーA110側に配送するなどのように、各ルーターに対してトラフィック配送の制御を行わせるようにしてもよい。

【0019】詳細に説明すると、まず、トラフィック測定装置115は、ネットワーク113を通過するデータの発信元IPアドレスと発信先IPアドレスとデータ量とを、所定の時間毎に測定する。例えば、図2に示すように、2秒毎に上記内容を測定し、IPアドレスが「10.XX.XX.XX」のWebサーバー111に対して送信されたデータ量と、このデータの送信元のIPアドレス「223.00.00.00」とを検出する。

【0020】トラフィック監視装置116では、トラフィック測定装置115が検出した結果の中で、データ量が設定されている値より大きい場合、ユーザーA110のWebサーバー111がネット攻撃を受けていると判断する。トラフィック監視装置116は、ネット攻撃と判断したら、ルーター制御装置103に、IPアドレス「223.00.00.00」からネット攻撃を受けている旨を通知する。

【0021】この通知により、ルーター制御装置103では、IPアドレス「223.00.00.00」から送信されてくるデータを、回線ルーター101やインターネットルーター102で破棄させるように制御する。ルーター制御装置103の制御の結果、インターネット130上のIPアドレス「223.00.00.00」から送信されてくるデータは、ユーザーA110に到達することが無く、Webサーバー111に対するネット攻撃は解消されることになる。

9

【0022】以下、本発明の通信状態制御方法に関して、図3のフローチャートを用いて説明する。まず、トラフィック測定装置115がネットワーク113における通信状態を測定し（ステップS2）、測定した通信状態をトラフィック監視装置116が判断する（ステップS3）。これらは、所定の一定時間毎に行う（ステップS1）。この判定では、自身のネットワーク113の例えばWebサーバー111に対する特定のIPアドレスからのデータ量が、規定値を超えたかどうかを判定する。ステップS3の判定で、特定のIPアドレスからのデータ量が規定値を超えたと判定した場合、トラフィック監視装置116は、ルーター制御装置103に対して、特定のIPアドレスからの攻撃が、IPアドレス「10.XX.XX.XX」のWebサーバー111に対して発生したことを通知する（ステップS4）。

【0023】トラフィック監視装置116から攻撃発生の通知を受けたルーター制御装置103は、回線ルーター101およびインターネットルーター102の動作を制限し、指定されたIPアドレスからのデータを破棄させる。この後、ルーター制御装置103は、破棄しているデータ量を監視し（ステップS7）、単位時間あたりの破棄データ量が規定値以下となったら、回線ルーター101およびインターネットルーター102の動作制限を解除する（ステップS8）。これらは、一定時間毎に行う（ステップS6）。

【0024】なお、上記実施の形態では、トラフィック測定装置115で測定したネットワーク113を通過するデータの発信元IPアドレスと発信先IPアドレスとデータ量とをともに、ユーザーのサーバーに対する攻撃を判断するようにしたが、これに限るものではない。トラフィック監視装置116で、Webサーバー111やメールサーバー112から、図4（a）に示すような、ネットワーク113に対して送信されてきたデータ量とこのデータの送信元などの情報、加えて、図4（b）に示すような、各サーバーにおける単位時間あたりのCPU稼働率、主メモリ使用率、一定時間あたりの接続数（総トラフィック）、単位時間あたりの通信量（トラフィック）を取得し、これら情報をもとに判断をするようにしてもよい。通信量の取得は、例えば、サーバーがネットワークに接続するためのインターフェース（NIC）を通過している通信量を、各サーバーから取得するようにすればよい。

【0025】例えば、上記CPUの稼働率と主メモリの使用率とサーバーに対する単位時間あたりのリクエスト数とサーバーに対する単位時間あたりの通信量とのいずれもが、図4（c）に示すような予め設定されている規定値を超えたら、ネット攻撃を受けていると判定するようにしてもよい。この判定の場合、ネット攻撃を受けていると判定した時点においてアクセスしている送信元のIPアドレスが、ネット攻撃をしている攻撃元とし、ト

10

ラフィック監視装置116は、この情報をルーター制御装置103に送信する。この結果、ルーター制御装置103は、回線ルーター101とインターネットルーター102とを制御し、上記IPアドレスからの送信データを破棄させる。

【0026】また、上記実施の形態では、トラフィック監視装置116で、ネット攻撃の発生有無を判定したが、これに限るものではなく、ルーター制御装置103でネット攻撃の発生有無を判定してもよい。この場合、トラフィック監視装置116は、トラフィック測定装置115が測定した結果や、トラフィック監視装置116が取得した情報を、ルーター制御装置103に送信し、トラフィック監視装置116から送られてきた情報をもとに、ルーター制御装置103が判定とルーター制御を行う。

【0027】ルーター制御装置103が判定を行う場合に関して、図5のフローチャートを用いて説明する。まず、トラフィック測定装置115がネットワーク113における通信状態を測定し（ステップS52）、測定した通信状態をトラフィック監視装置116が、ルーター制御装置103に送信する（ステップS53）。次いで、データを受信したルーター制御装置103は、受け取った通信状態からネット攻撃の有無を判定する（ステップS53）。これらは、一定時間毎に行う（ステップS51）。この判定では、通信状態を送信してきたユーザーA110のネットワーク113のWebサーバー111に対する特定のIPアドレスからのデータ量が、規定値を超えたかどうかを判定する。

【0028】ステップS53の判定で、特定のIPアドレスからのデータ量が規定値を超えたと判定した場合、ルーター制御装置103は、回線ルーター101およびインターネットルーター102の動作を制限し、規定値を超えたデータ量を送信してきたIPアドレスからのデータを破棄させる（ステップS55）。この後、ルーター制御装置103は、破棄しているデータ量を監視し（ステップS57）、単位時間あたりの破棄データ量が規定値以下となったら、回線ルーター101およびインターネットルーター102の動作制限を解除する（ステップS58）。これらは、一定時間毎に行う（ステップS56）。

【0029】

【発明の効果】以上説明したように、本発明によれば、一定量以上のデータを送信してきた送信元からのデータの送信が、ISPにおいて破棄されるので、大量のデータを送信してくる不正アクセスから、ISPに接続されているユーザーのサーバーを守れるという優れた効果が得られる。

【図面の簡単な説明】

【図1】 本発明の実施の形態における通信状態制御システムの構成を示す構成図である。

11

【図2】 トラフィック測定装置の測定結果の一例を示す図である。

【図3】 本発明の実施の形態における通信状態制御方法を示すフローチャートである。

【図4】 トラフィック監視装置の取得したデータの一例を示す図である。

【図5】 本発明の他の形態における通信状態制御方法を示すフローチャートである。

【図6】 従来のISPを介してインターネットに接続*

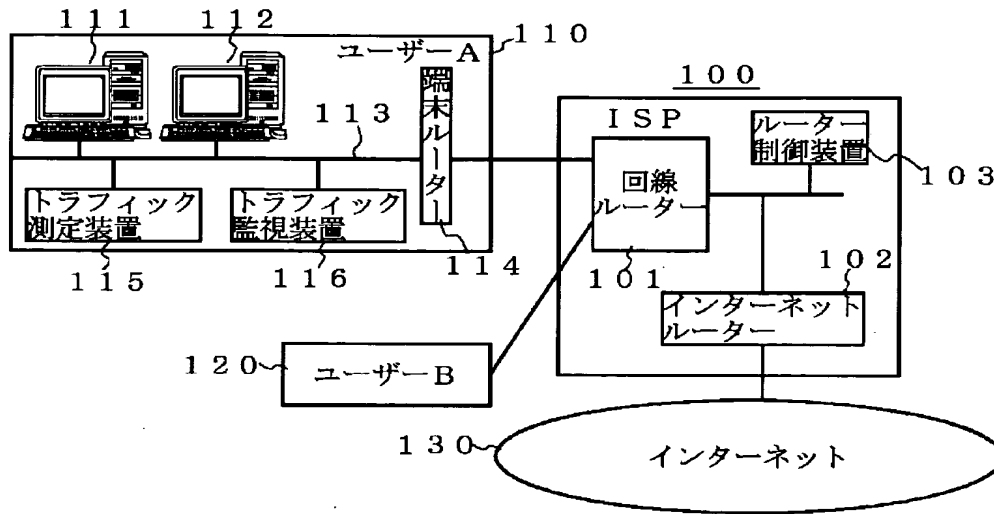
12

*する形態を示す構成を示す構成図である。

【符号の説明】

100…ISP (Internet Service Provider)、101…回線ルーター、102…インターネットルーター、103…ルーター制御装置、110…ユーザーA、111…Webサーバー、112…メールサーバー、113…ネットワーク、114…端末ルーター、115…トラフィック測定装置、116…トラフィック監視装置、120…ユーザーB、130…インターネット。

【図1】

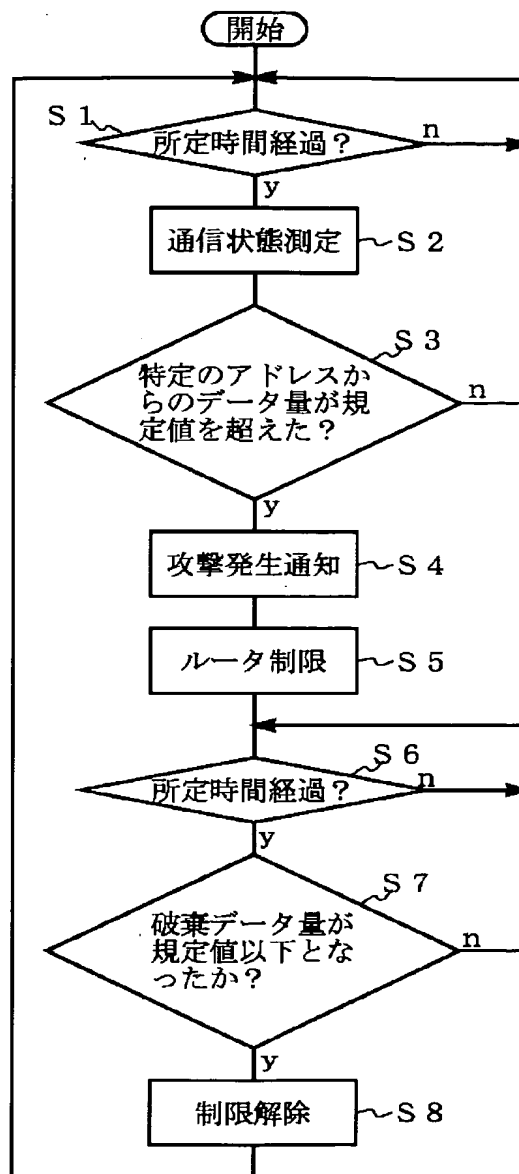


【図2】

アクセス時刻	送信元 IPアドレス	受信先 IPアドレス	データ量	...
2000/4/18 18:45:00	10.XX.XX.XX	233.XX.XX.XX	〇〇〇	...
	11.XX.XX.XX	234.XX.XX.XX	〇〇〇	...

2000/4/18 18:45:02	10.XX.XX.XX	223.XX.XX.XX
	11.XX.XX.XX	224.XX.XX.XX

【図3】



【図4】

(a)

アクセス時刻	送信元IPアドレス	データ量	DNS情報
2000/4/18 18:45:00	234.XX.XX.XX	〇〇〇	□□□
	233.XX.XX.XX	〇〇〇	□□□

2000/4/18 18:45:02	234.XX.XX.XX	△△△
	233.XX.XX.XX	△△△

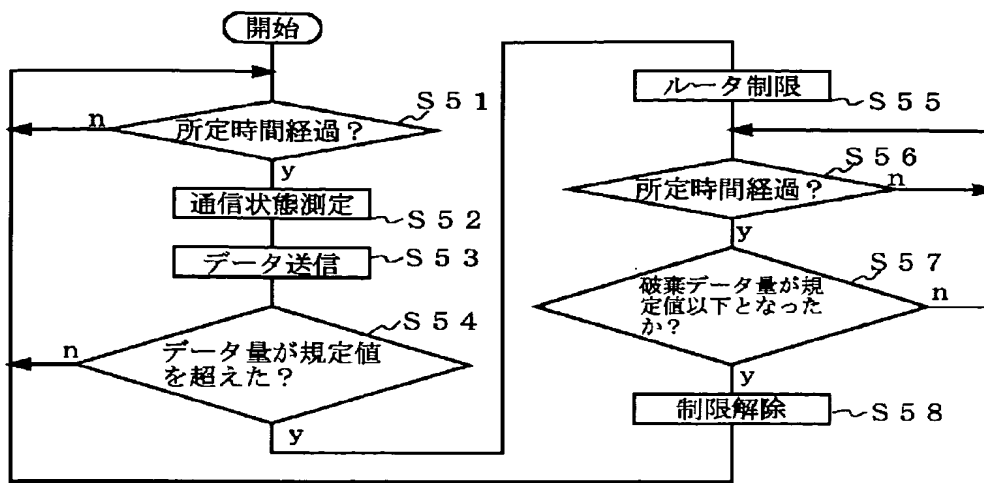
(b)

監視項目 対象	単位時間あたりの CPU稼働率	単位時間あたりの メモリ稼働率	一定時間あたりの 総トラフィック	単位時間あたりの トラフィック
Webサーバ	25	15	225550	185
端末ルータ	50	50	1258822	352
.
.
.
.

(c)

	Webサーバ	端末ルータ	.	.
単位時間あたりの CPU稼働率	85	82	.	.
単位時間あたりの メモリ稼働率	98	98	.	.
一定時間あたりの 総トラフィック	3000000	25000000	.	.
単位時間あたりの トラフィック	500	5000	.	.
一定、単位時間あたりの トラフィック(特定送信元IPアドレス)	1200000	5000000	.	.
	380	3500	.	.
.

【図5】



【図6】

